Regional Shifts in Cybersecurity Talent An In-Depth View with the NICE Framework

Key Takeaways

- Since 2022, LinkedIn has been working closely with the NICE program of the National Institute of Standards and Technology (NIST) under the U.S. Department of Commerce. Together, they worked to create a crosswalk between cybersecurity job positions identified by LinkedIn and Work Role categories from the NIST Special Publication 800-181r1, NICE Workforce Framework for Cybersecurity (NICE Framework). The NICE Framework Work Role Categories bring a clearer view of what cybersecurity roles are in demand and where talent already exists. The crosswalk allows for standardized national and international measurements of the cybersecurity workforce, demand, and overall composition.
- There are seven NICE Framework Work Role categories that organize the framework's 52 Work Roles: Oversight and Governance, Design and Development, Implementation and Operation, Protection and Defense, Investigation, Cyberspace Intelligence, and Cyberspace Effects.
- Nationally, the composition of cybersecurity talent and job postings has
 remained largely stable. The Work Role category with the greatest increase
 in share of cybersecurity talent is Protection and Defense (+0.5% year over
 year from April 2023 to April 2024). The Work Role category with the
 greatest increase in share of cybersecurity job postings is Implementation
 and Operation (+1.2% year over year from April 2023 to April 2024).
- At the state level, there are larger shifts in the composition of talent and demand for specific Work Role categories. Some of the largest increases in the share of cybersecurity job postings are for Implementation and Operation in Alaska (+19.9%), Oversight and Governance in North Dakota (+16.2%) and Implementation and Operation in Iowa (+12.5%).

Caroline Liongosari

Data Scientist
Economic Graph
Research Institute
cliongosari@linkedin.com

Akash Kaura

Staff Data Scientist Economic Graph Research Institute akaura@linkedin.com



LinkedIn and NICE

Starting in 2022, LinkedIn's Economic Graph Research Institute worked closely with the NICE program of the National Institute of Standards and Technology (NIST) under the U.S. Department of Commerce to analyze workforce and hiring trends in the cybersecurity space. NIST Special Publication 800-181 Rev. 1, the NICE Workforce Framework for Cybersecurity (NICE Framework) establishes a common language to describe cybersecurity work that is used among public, private, and academic sectors. In March 2024, NICE released version 1.0.0 of the NICE Framework Components, which included an update to the Work Roles and their categories; Competency Areas, and the Task, Knowledge, and Skill (TKS) statements that they comprise.

For this report and our broader cybersecurity research efforts, Linkedln worked with NICE to create a crosswalk between jobs Linkedln members list on their Linkedln profiles and the 52 Work Roles and their associated categories to identify areas of demand and to determine where cybersecurity talent for each category already exists. This crosswalk now allows us to consistently identify relevant cybersecurity talent and jobs, compare across various cities, states, and countries, and understand trends over time.

Creating the LinkedIn Jobs / NICE Framework Crosswalk

The NICE Framework consists of 52 Work Roles organized into seven Work Role categories¹:

- 1. Oversight and Governance: Provides leadership, management, direction, and advocacy so the organization may effectively manage cybersecurity-related risks to the enterprise and conduct cybersecurity work.
- 2. Design and Development: Conduct research, conceptualizes, designs, develops, and tests secure technology systems, including on perimeter and cloud-based networks.
- 3. Implementation and Operation: Provides implementation, administration, configuration, operation, and maintenance to ensure effective and efficient technology system performance and security.
- 4. Protection and Defense: Protects against, identifies, and analyzes risks to technology systems or networks. Includes investigation of cybersecurity events or crimes related to technology systems and networks.
- 5. Investigation: Conducts national cybersecurity and cybercrime investigations, including the collection, management, and analysis of digital evidence.
- 6. Cyberspace Intelligence: Collects, processes, analyzes, and disseminates information from all sources of intelligence on foreign actors' cyberspace programs, intentions, capabilities, research and development, and operational activities.

August 2024

¹ NICE Framework Components v1.0.0

7. Cyberspace Effects: Plans, supports, and executes cyberspace capabilities where the primary purpose is to externally defend or conduct force projection in or through cyberspace.

Work Roles that fall under each category were used to match jobs Linkedln members list in their profiles through the following rule-based approach:

- 1. String matching NICE Framework Work Role Categories that clearly matched Linkedln jobs.
- 2. String matching NICE Framework Work Roles to raw LinkedIn job titles, which are then matched to corresponding job families.
- 3. Match remaining cybersecurity job families through techniques such as LinkedIn's Skills Genome to match with one or more NICE Framework Work Role categories.
- 4. Finalize the crosswalk with final review with NICE program staff.

In step three, we utilize thresholds (based on proportion of members, etc.) and similarity measures based on the LinkedIn skills genome² for a given occupation to get the most representative skills per occupation.

Using the finalized crosswalk, we first show the most common US job titles held by LinkedIn members for each NICE Framework Work Role category below for the past five years (2019-2024) below. We also note that it is possible for a job title to equate to one or more roles. To understand more, see NICE's explanation here.

Top 5 Most Common Job Titles by NICE Framework Work Role Category

NICE Work Role Category	Rank 1 Job Title	Rank 2 Job Title	Rank 3 Job Title	Rank 4 Job Title	Rank 5 Job Title
Design and Development	Software Engineer	Security Engineer	Enterprise Architect	Information Security Engineer	Security Architect
Implementation and Operation	Network Engineer	Cybersecurity Analyst	Security Analyst	Network Analyst	Network Security Engineer
Oversight and Governance	System Administrator	Security Manager	Chief Information Security Officer	Security Consultant	Program Manager
Protection and Defense	Security Engineer	Cyber Security Analyst	Cyber Security Engineer	Security Analyst	Chief Information Security Officer

Source: LinkedIn Economic Graph

August 2024

² LinkedIn Engineering Blog: <u>How we mapped the "skills genome" of emerging jobs</u>

The NICE Framework Work Role categories of Cyberspace Effects, Cyberspace Intelligence, and Investigation comprise Work Roles typically carried out by U.S. military forces and federal intelligence and law enforcement agencies. Because some Work Roles in these categories do not appear in sufficient volume in our data, they are not reported here.

The Composition of Cybersecurity Talent and Demand Remains Stable Nationally

In the past year, we find that the composition of the cybersecurity workforce in the US by NICE Framework Work Role category has not changed significantly between April 2023 and April 2024, moving by less than 5pp in year-over-year (YoY) terms. The largest change has been in the Protection and Defense category (+0.5pp).

Composition of the US Cybersecurity Workforce by NICE Framework Work Role Category

NICE Work Role Category	April-23	April-24	YoY% Change
Protection and Defense	25.3%	25.8%	0.5%
Design and Development	19.3%	19.4%	0.2%
Implementation and			
Operation	23.0%	22.9%	-0.1%
Oversight and Governance	30.2%	29.7%	-0.4%

Similarly, we also do not see major changes in the national-level composition of cybersecurity job postings. The NICE Work Role category with the greatest change in job postings nationally is Implementation and Operation with a 1.2% increase between April 2023 and April 2024.

Composition of the US Cybersecurity Job Postings by NICE Framework Work Role Category

NICE Work Role Category	April-23	April-24	YoY% Change
Implementation and			
Operation	21.9%	23.0%	1.2%
Oversight and Governance	22.4%	22.5%	0.2%
Design and Development	25.6%	25.0%	-0.6%
Protection and Defense	28.8%	28.1%	-0.7%

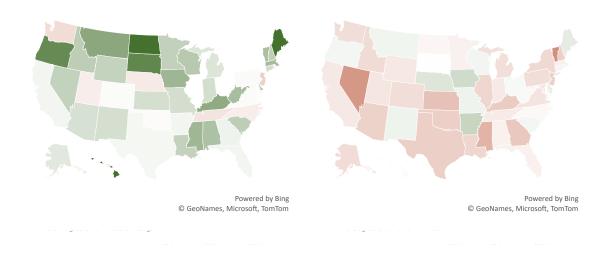


Regional Cybersecurity Talent and Demand Varies

While at the national level the composition of the cybersecurity workforce and job postings is very stable, we see more variation at the state level.

I. Oversight and Governance

YoY% Change in Oversight & Governance Job Postings and Workforce as of April 2024



Source: LinkedIn Economic Graph

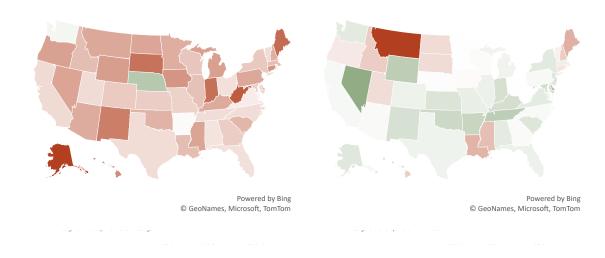
North Dakota (16.2%), Hawaii (12.1%), and Maine (11.3%) lead the way in having the greatest YoY% increase in the share of job postings in the Oversight and Governance category out of all cybersecurity job postings. The states/regions with the greatest decrease are New Jersey (-2.5%), Washington D.C (-1.9%) and Washington (-1.8%).

The states with the greatest increase in the share of their cybersecurity workforce associated with the Oversight and Governance category are Arkansas (2.9%), lowa (2.5%), and Nebraska (1.8%) while the states with the greatest decrease are Vermont (-5.9%), Nevada (-5.4%), and Mississippi (-3.9%).



II. Design and Development

YoY% Change in Design & Development Job Postings and Workforce as of April 2024



Source: LinkedIn Economic Graph

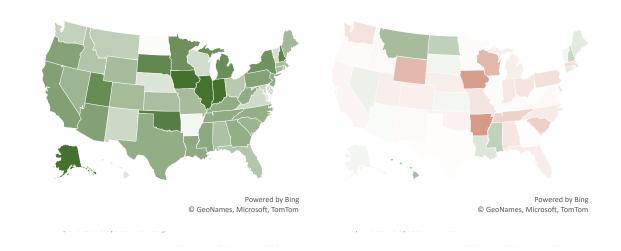
For jobs most closely aligned with Work Roles in the Design and Development category, we mostly see a decline in share of cybersecurity job postings, while a few US states have increases in share of cybersecurity job postings including Nebraska (3.9%), Washington (0.7%), and Arkansas (0.3%). The states with the greatest decrease of job postings in this category are Alaska (-11.7%), West Virginia (-8.5%), and Maine (-7.7%).

Despite the decrease in job postings, however, we see an increase in talent in Design and Development category. The three states with the greatest YoY% increase in the share of the state's cybersecurity workforce in this category are Nevada (5.8%), Delaware (4.2%), and Nebraska (3.9%). The states with the largest decreases are Montana (-15.9%), Maine (-4.1%) and Louisiana (-3.9%).



III. Implementation and Operation

YoY% Change in Implementation & Operation Job Postings and Workforce as of April 2024



Source: LinkedIn Economic Graph

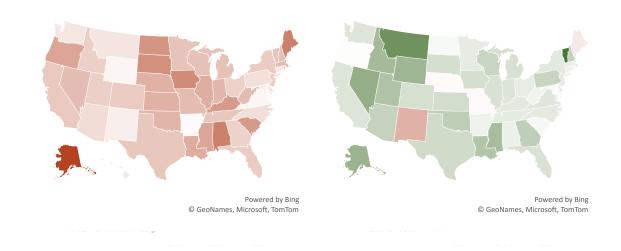
All US states have seen an increase in the share of job postings in the Implementation and Operation Work Role category. However, a few states stand out in their increased demand for Implementation and Operation talent with Alaska (19.9%), Iowa (12.5%), and Indiana (10.3%) having double-digit YoY% increases in the share of cybersecurity job postings. The states and regions with the lowest YoY% increase are North Dakota (0.2%), Arkansas (0.7%) and Hawaii (1.7%).

Despite the increase in demand for Implementation and Operation talent, we do not see a similar pattern in the growth of their workforce in all US states. The states with the greatest increase in the share of Implementation and Operation workforce are Hawaii (4.7%), Montana (4.7%), and North Dakota (3.3%). The states with the largest decrease are Arkansas (-5.3%), lowa (-5.1%), and Wisconsin (-3.7%).



IV. Protection and Defense

YoY% Change in Oversight & Governance Job Postings and Workforce as of April 2024



Source: LinkedIn Economic Graph

We see a major decrease in the share of cybersecurity job postings for Protection and Defense in all US states except for Hawaii (1.9%) and Washington DC (0.1%). The states with the largest decreases are Alaska (-9.9%), Maine (-6.6%), and Alabama (-6.6%).

The states with the largest increase in the share of cybersecurity workforce in Protection and Defense are Vermont (9.7%), Montana (7.7%), and Nevada (5.7%). The ones with largest decreases are New Mexico (-4.0%), Delaware (-1.7%), and Maine (-1.1%).

Final Thoughts

As noted in a previous report³, cybersecurity talent demand in the US has cooled in the past year. Through this report's analyses of demand composition, however, we find the picture of the cybersecurity talent marketplace to be more nuanced. Several regions are seeing growing demand for specific cybersecurity roles and declining in other areas. Stay tuned for more updates from the Economic Graph Research Institute at our microsite.

Acknowledgements

³ Cybersecurity Trends in the US (April 2024)

The LinkedIn Economic Research Institute is grateful to NICE – specifically <u>Karen Wetzel</u> and <u>Michael Prebil</u> for their ongoing collaboration in helping us bring out the latest cybersecurity and workforce trends in the US through the development of the LinkedIn Occupation – NICE Framework crosswalk. While nationally we did not see major shifts in the makeup of cybersecurity talent demand or talent by NICE Work Role category, we did find shifts at the state-level. These state-wide shifts help inform employers determine their next best course of action to hire or attract talent at a more local level. It also informs cybersecurity talent to determine where their expertise and skills are most in demand.

Methodology

- Our work represents the world seen through LinkedIn data, drawn from the anonymized and
 aggregated profile information of LinkedIn's one billion members around the world. As such, it is
 influenced by how members choose to use the platform, which can vary based on professional,
 social, and regional culture, as well as overall site availability and accessibility. In publishing
 these insights from LinkedIn's Economic Graph, we want to provide accurate statistics while
 ensuring our members' privacy. As a result, all data show aggregated information for the
 corresponding period following strict data quality thresholds that prevent disclosing any
 information about specific individuals.
- Data in this report focuses on the United States only.
- We have included data from 2019 onwards in this analysis.
- Members are considered 'Cybersecurity Professionals' if they hold one of the NICE Frameworkaligned LinkedIn Occupations that we have identified as being Cybersecurity related. Their NICE Work Role category is assigned based on the occupation they hold and is mapped with the LinkedIn Occupation – NICE Framework crosswalk.